ArticSoft OpenPGP Command Line Scriptor

Automatically encrypt, sign, decrypt, verify, archive, email, FTP and securely delete files – no user interaction required

Command Line Scriptor (CLS) is a simple to use, non-interactive utility that lets you specify security actions from the command line. Actions can scheduled to occur straight away or at a specific date/time. Once the command line parameters have been setup CLS runs on it's own without any further user interaction.

Unlike other command line products, CLS lets you define your command line parameters through the use of a simple GUI so all the hard work of setting up complex commands is done for you. More advanced users can always type the required parameters directly on the command line or save them in a file for later processing by CLS.

Full OpenPGP and PKI compatibility ensure complete integration with existing systems (PGP, GnuPGP, etc.).

The following commands can be specified :

Outgoing

- Which files / folders to encrypt
- Who you want to encrypt them for
- Encrypt multiple files/folders into an archive (zip file)
- Send files / archives by email
- Upload / download files by FTP
- Securely delete source files after encryption
- Digitally sign files / archives
- When you want these actions to occur [date/time]
- Where encrypted/signed files should be stored
- Whether existing encrypted files should be overwritten

Incoming

- Which files / folders / archives to decrypt
- Which files / folders / archives to verify
- Where decrypted/verified files should be stored
- Whether existing files should be overwritten
- When you want these actions to occur [date/time]

Wild cards are accepted so you can decrypt and verify all incoming files with a specific extension (say *.pgp) in a given folder(s) or encrypt all files with a specific extension (say *.xls) in a given folder(s).

Key Generation & Management

CLS's key manager lets you generate your own X.509 and OpenPGP compliant certificates and keys, or you can import them from any Certificate Authority (VeriSign, GeoTrust, etc.) or OpenPGP compliant product. Its backup and restore facility and password changer ensure you have full control over the management of your keys. For the more technically minded, advanced key information is just a single click away.

Its unique Trusted Authorities system shields you from the complexities of importing Root Certificates in order to verify keys. Keys signed by all the major Certificate Authorities are automatically recognized. Notes can be added to every key you generate or import to help you identify keys or to store additional information that you want associated with them.

CLS automatically interacts with the keystore when cryptographic functions are required.

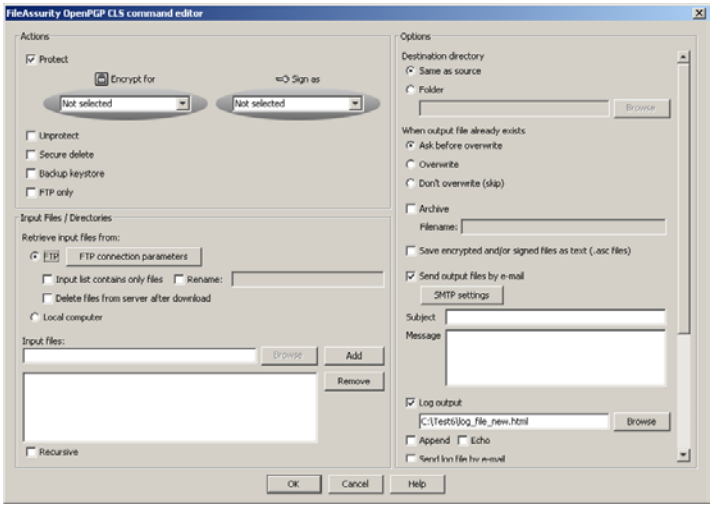

Diagram 1: Command Line Scriptor GUI

Automated Secure Email

When emailing files CLS automatically determines who they are to be sent to by using the email addresses contained in the public keys. CLS uses SMTP to send emails.

At the receiving end FileAssurity OpenPGP, our free reader software, CLS, or any other OpenPGP compliant software can be used to decrypt the secured files.

Automated FTP

After protection of files CLS can automatically FTP them to your designated web server. You can even schedule CLS to check every x minutes or hours for protected or unprotected files and have them downloaded and unprotected / protected all in one simple operation (and then automatically uploaded to the server again if required).

ARTICSOFT

Comprehensive Audit Trail

A report on the actions that occurred and full error reporting is written to a log file. Who information was encrypted for, who it was sent to and when this occurred, etc. is automatically recorded when command line parameters are run.

The audit trail shows you :

- what command line parameters you specified
- when they were executed [date/time]
- files that were affected
- what occurred (encryption, digital signing, etc.)
- the order that this occurred in (e.g encrypted *.doc to *.pgp, then securely deleted *.doc in c:\temp)
- keys that were used
- any errors that were encountered

You can specify the location of the log file and whether reports can be written to the same log file or to a new file each time the command line parameters are run. Any errors are written to the log file and/or can be written to the screen or emailed.

Features & Benefits

- Complete automation of cryptographic functions with date and time scheduling
- Simple to use – GUI based generation of command line parameters and script testing
- Quick to install and setup
- Built in key management
- Uses public key technology - full strength protection and no exchange of passwords required
- Extremely flexible – can be used in any type of industry – the possibilities are endless
- Ultra secure – recipient email addresses are taken from the information contained in the public keys so no spoofing can occur
- No user intervention required
- Comprehensive auditing and error reporting
- Provides automatic verification and decryption for incoming forms protected by FormsAssurity
- Provides automatic verification and decryption for incoming files protected by any OpenPGP compliant software
- Built-in FTP client, including automatic renaming and remote deletion of files
- Supports any application that's output can run in a shell
- Auto logon and multi-processing of commands

Uses for Command Line Scriptor

Medical

Files being sent to a transcription agency can be automatically encrypted and then e-mailed or made available for FTP upload to a web server. At the transcription agency encrypted files can be automatically checked for having come from an approved source and can be automatically decrypted for the end user to work on.

Billing or debt collection e-mails can be automatically encrypted and then e-mailed to the appropriate agency without any user involvement.

Banking

Customer statements can be automatically encrypted for customers so that they are never exposed whilst sitting on servers or being transferred to an ISP for forwarding. Complete end-to-end protection without the risk of hackers capturing personal information.

Insurance

Used in conjunction with FormsAssurity, insurers can automatically verify digitally signed and encrypted claims forms sent by customers and agents using standard web forms, avoiding possible exposure of personal details and guaranteeing confidentiality of information. Information to agents and representatives can be routinely encrypted for e-mail transmission without the need for VPN or other technologies.

Commerce

Orders, confidential price lists, company financial and corporate governance reports and similar information can be automatically encrypted and mailed to investors, key customers and suppliers without any risk of loss or exposure if they are intercepted or delivered to the wrong person in error.

Technical Information	
Signing Algorithm	RSA 2048 bit, DH/DSS 1024/2048 bit
Hashing Algorithm	SHA-1 (160 bit), MD5 supported
Encryption Algorithm	AES (256 bit)
Platforms supported	Windows NT, 2000, 2003, XP
Computer requirements	Pentium II Processor, 128MB RAM
Certificate formats supported	PKCS#7, .P7B, .CER, .P12, .PFX, X.509, .PGP, .GPG, .ASC

ARTICSOFT